IN THE CLAIMS

1. (Currently Amended)   A method of validating software for hardware, comprising:

authenticating a certificate from a code image with a first public key, the code image including the software;

obtaining a signature generated for the software from the code image, a first identifier for the software, and a second identifier for the hardware, wherein the signature is generated using cryptography and is used to validate an association of the software with the hardware; and

validating the signature with a second public key from the certificate, wherein the association of the software with the hardware is validated if the signature is validated.

2. (Original)   The method of claim 1, wherein the software is executed by the hardware only if the association is validated.

3. (Original)   The method of claim 1, wherein the validating the signature includes

hashing information for the software, the first identifier, and the second identifier to obtain a first digest,

decrypting the signature with the second public key to obtain a second digest, and

comparing the first digest against the second digest, and wherein the signature is validated if the first digest matches the second digest.

4. (Original)   The method of claim 3, wherein the validating the signature further includes

hashing the software to obtain a third digest used as the information for the software.

5. (Original)   The method of claim 1, wherein the signature is generated using a cryptography scheme that includes Hash-based Message Authentication Code (HMAC).

6. (Original)   The method of claim 1, wherein the first identifier is a software release version number.

7. (Original)   The method of claim 1, wherein the hardware is an integrated circuit of a specific design.

8. (Original)   The method of claim 1, wherein the second identifier is a hardware serial number or a part number.

9. (Currently Amended)   An apparatus operable to validate software for hardware, comprising:

a first storage unit configured to store a first public key; and

a processor operative to

authenticate a certificate <u>from a code image</u> with the first public key, <u>where the code image includes the software,</u>

obtain a signature generated for the software<u> from the code image</u>, a first identifier for the software, and a second identifier for the hardware, wherein the signature is generated using cryptography and is used to validate an association of the software with the hardware, and

validate the signature with a second public key from the certificate, wherein the association of the software with the hardware is validated if the signature is validated.

10. (Original) The apparatus of claim 9, wherein the first storage unit is further configured to store the second identifier for the hardware, and wherein the processor is further operative to

hash information for the software, the first identifier, and the second identifier from the first storage unit to obtain a first digest,

decrypt the signature with the second public key to obtain a second digest, and

compare the first digest against the second digest, and wherein the signature is validated if the first digest matches the second digest.

11. (Original) The apparatus of claim 9, further comprising:

a second storage unit configured to store boot code executed by the processor to authenticate the certificate and validate the signature.

3

12. (Original) The apparatus of claim 11, wherein the first and second storage units and the processor are implemented within an integrated circuit.

13. (Original) The apparatus of claim 9 and implemented within a wireless communication device.

14. (Currently Amended)   An apparatus operable to validate software for hardware, comprising:

means for authenticating a certificate sent with a code image including the software using with a first public key;

means for obtaining a signature generated for the software and sent with the code image, a first identifier for the software, and a second identifier for the hardware, wherein the signature is generated using cryptography and is used to validate an association of the software with the hardware; and

means for validating the signature with a second public key from the certificate, wherein the association of the software with the hardware is validated if the signature is validated.

15. (Original) The apparatus of claim 14, wherein the means for validating the signature includes

means for hashing information for the software, the first identifier, and the second identifier to obtain a first digest,

means for decrypting the signature with the second public key to obtain a second digest, and

means for comparing the first digest against the second digest, and wherein the signature is validated if the first digest matches the second digest.

16. (Currently Amended)   A method of associating software with hardware, comprising:

obtaining a first identifier for the software;

obtaining a second identifier for the hardware, the second identifier identifying a non-specific hardware platform; and

generating a first signature for the software, the first identifier, and the second identifier using cryptography, wherein the first signature is used to validate an association of the software with the hardware,

receiving a digest obtained by hashing the software, and wherein the first signature is generated over the digest, the first identifier, and the second identifier.

17. (Cancel)

18. (Original) The method of claim 16, wherein the first signature is generated using a cryptography scheme that includes Hash-based Message Authentication Code (HMAC).

19. (Original) The method of claim 16, further comprising:

providing a certificate containing a first public key and a second signature, the first public key corresponding to a first private key used to generate the first signature, and the second signature being generated over the first public key with a second private key for an entity generating the second signature.

20. (Original) The method of claim 16, further comprising:

receiving from an entity a request for the first signature; and

authenticating the entity prior to generating the first signature.

21. (Original) The method of claim 16, further comprising:

determining whether or not association of the software with the hardware is permitted, and wherein the first signature is generated only if the association is permitted.

22. (Original) The method of claim 21, wherein the determining is based on a configuration table of permitted associations between at least one version of software and at least one platform of hardware.

23. (Previously Presented)   An apparatus operable to associate software with hardware, comprising:

a communication unit operative to obtain, from a code generator entity, information for a software code, a first identifier for the software, and a second identifier for the hardware; and

a controller operative to generate a signature for the software, the first identifier, and the second identifier using cryptography and a first secure cryptographic key, wherein the signature is used to validate an association of the software with the hardware, the controller further configured to generate a certificate using a second secure cryptographic key, the certificate used to authenticate a certificate authority.

24. (Original) The apparatus of claim 23, wherein the controller is further operative to determine whether or not association of the software with the hardware is permitted, and to generate the signature only if the association is permitted.

25. (Original) The apparatus of claim 23, wherein the controller is further operative to authenticate the code generator entity prior to generating the signature.

26. (Original) The apparatus of claim 23, further comprising:

a memory unit operative to store a configuration table of permitted associations between at least one version of software and at least one platform of hardware, and wherein the controller is further operative to determine whether or not the association of the software with the hardware is permitted based on the configuration table.

27. (Previously Presented) An apparatus operable to associate software with hardware, comprising:

means for obtaining a first identifier for the software;

means for obtaining a second identifier for the hardware;

means for receiving a digest obtained by hashing the software;

means for generating a first signature for the software, based on the digest, the first identifier, and the second identifier using cryptography and a first secure cryptographic key, wherein the first signature is used to validate an association of the software with the hardware; and

means for generating a certificate associated with the first signature using cryptography and a second secure cryptographic key, wherein the certificate is used to authenticate a certificate authority.

28. (Original) The apparatus of claim 27, further comprising:

means for receiving from an entity a request for the first signature; and

means for authenticating the entity prior to generating the first signature.

29. (Previously Presented)   A method of associating software with hardware, comprising:

providing information for the software;

providing a first identifier for the software;

providing a second identifier for the hardware;

receiving a signature generated for the software, the first identifier, and the second identifier, wherein the signature is generated using cryptography and a first secure cryptographic key, and is used to validate an association of the software with the hardware;

receiving a certificate containing cryptographic information used to validate the signature, the certificate generated using cryptography and a second secure cryptographic key; and

forming an image comprised of the software, the signature, and the certificate.

30. (cancel)

31. (Previously Presented)   The method of claim 29, wherein the signature is generated using a cryptography scheme that includes Hash-based Message Authentication Code (HMAC), and wherein the HMAC receives the first digest, the first identifier, and the second identifier as inputs and provides a second digest used to generate the signature.

32. (Previously Presented)   An apparatus operable to associate software with hardware, comprising:

a communication unit operative to

provide information for the software, a first identifier for the software, and a second identifier for the hardware,

receive a signature generated for the software, the first identifier, and the second identifier, wherein the signature is generated using cryptography and a first secure cryptographic key, and is used to validate an association of the software with the hardware, and

receive a certificate containing cryptographic information used to validate the signature, the certificate generated using cryptography and a second secure cryptographic key; and

a controller operative to form an image comprised of the software, the signature, and the certificate.

33. (canceled)

34. (Previously Presented)   An apparatus operable to associate software with hardware, comprising:

means for providing information for the software;

means for providing a first identifier for the software;

means for providing a second identifier for the hardware;

means for receiving a signature generated for the software, the first identifier, and the second identifier, wherein the signature is generated using cryptography and a first secure cryptographic key, and is used to validate an association of the software with the hardware;

means for receiving a certificate containing cryptographic information used to validate the signature, the certificate generated using cryptography and a second secure cryptographic key; and

means for forming an image comprised of the software, the signature, and the certificate.

35. (canceled)

36. (New) An apparatus operable to validate software for hardware, comprising:

a storage device configured to store a code image including the software, a code signature, and a certificate;

a secure storage device configured to store a hardware identifier and a certificate authority public key;

a processor configured to access the storage device and operative to:

authenticate the certificate with the certificate authority public key,

obtain a regenerated signature digest based on the software, a first identifier for the software, and the hardware identifier,

decrypt the certificate using the certificate authority public key to recover a code public key,

decrypt the code signature using the code public key to recover a received signature digest, and

compare the regenerated signature digest with the received signature digest to validate the association of the software with the hardware.